(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 June 2001 (28.06.2001)

PCT

(10) International Publication Number
WO 01/47176 A1

(51) International Patent Classification[7]: H04L 9/12, 9/08

(21) International Application Number: PCT/US00/42168

(22) International Filing Date:
13 November 2000 (13.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/461,519 14 December 1999 (14.12.1999) US

(71) Applicant: YODLEE.COM.INC. [US/US]; 3600 Bridge Parkway, 2nd Floor, Redwood Shores, CA 94065 (US).

(72) Inventors: SATYAYOLU, Ramakrishna; 3707 Poinciana Drive, Apt. 154, Santa Clara, CA 95051 (US). INALA, Suman, Kumar; 3707 Poinciana Drive, Apt. 154, Santa Clara, CA 95051 (US). SHAKHAR, Dimakar; 3707 Poinciana Drive, Apt. 154, Santa Clara, CA 95051 (US). RAJAN, Sreeranga, P.; 3475 Granada Avenue #320, Santa Clara, CA 95051 (US).

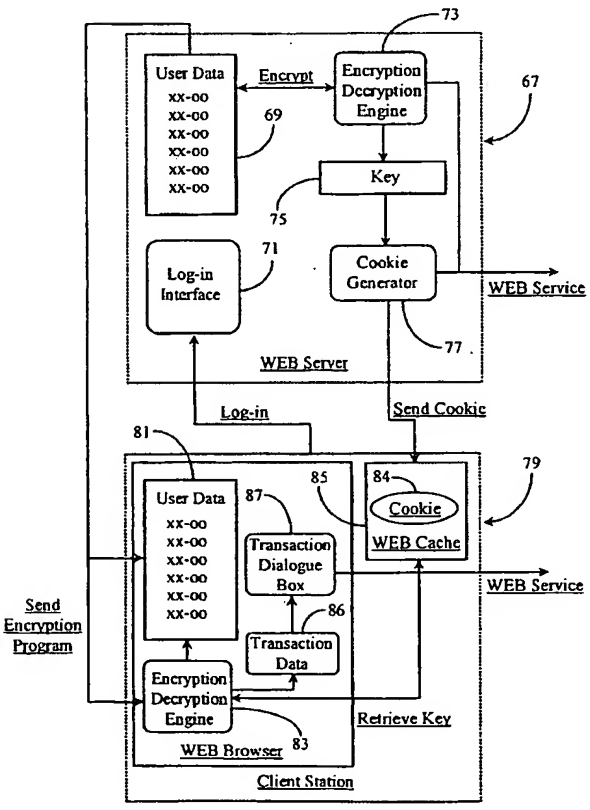
(74) Agent: BOYS, Donald, R.; P.O. Box 187, Aromas, CA 95004 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR A REVOLVING ENCRYPTING AND DECRYPTING PROCESS



(57) Abstract: Refering to figure 1, a scheme for encryption and decryption of data between two computer stations operating in the Internet environment uses a cookie sent by servers (67) to transmit a key (75) for encryption and decryption. The key (75) can be the cookie value, or the cookie value can contain or encompass the key (75) in some form known to both machines.The server (67) may encrypt data for a client (79) using a key (75) also sent to the client (79) in a cookie, and the client (79) may then retrieve the key (75) and use it for decrypting data sent. Server (67) may also use the scheme in a variation to encrypt data on a client (79) machine. Two servers may use the scheme as well. In some cases a copy of an encryption/decryption (83) engine is sent as well, and in some cases the copy sent is temporary.

WO 01/47176 A1

Published:

— *With international search report.*

— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Method and Apparatus for a Revolving Encrypting and Decrypting Process

Field of the Invention

The present invention is in the field of Internet navigation and secure log-in and transaction methods and pertains more particularly to methods and apparatus for encrypting and decrypting data that is routinely sent over a data-packet network from one computer to another.

Background of the Invention

The information network known as the world-wide-web (WWW), which is a subset of the well-known Internet, is arguably the most complete source of publicly accessible information available. Anyone with a suitable Internet appliance such as a personal computer with a standard Internet connection may access (go on-line) and navigate to information pages (termed web pages) stored on Internet-connected servers for the purpose of garnering information and initiating transactions with hosts of such servers and pages.

Many companies offer various subscription services accessible via the Internet. For example, many people now do their banking, stock trading, shopping, and so forth from the comfort of their own homes via Internet access. Typically, a user, through subscription, has access to personalized and secure WEB pages for such functions. By typing in a user name and a password or other personal identification code, a user may obtain information, initiate transactions, buy stock, and accomplish a myriad of other tasks.

There are many methods known in the art for providing measures of security for patrons of on-line services. Secure connections protected by firewalls, authenticated certificates authorizing senders of information, encryption methods, and others. Many of these methods fall short in one aspect or another of providing

complete security for an end user. For example, some encryption programs store both the program and key on an end user's station where an unauthorized user may compromise both. Many secure connections and servers are not completely immune from attack by computer hackers attempting to intercept and steal proprietary data. Some encryption and decryption programs may be undermined by a persistent hacker intent on solving the encryption scheme.

It has occurred to the inventor that sensitive information may be usurped even if encrypted and sent to a user's station for log-in. An unauthorized user may under certain circumstances find a decryption key on a user's station. Once found, the key may be used to decrypt and steal all sorts of sensitive encrypted data. Still a greater level of security must be observed for secure auto-logins and other sensitive transactions between servers and from servers to user stations.

What is clearly needed are more secure methods for encrypting and decrypting data transferred between computers.

Summary of the Invention

In a preferred embodiment of the present invention, in a client-server system, a method for encrypting and sending data from the server to the client and enabling decryption by the client is provided, comprising steps of (a) upon receiving a log-in and a data request from the client by the server, sending a cookie to the client, the cookie comprising a key value to be used for decrypting the data; (b) encrypting the data to be sent to the client using an encryption/decryption engine and the value of the key; and (c) sending the encrypted data to the client. There may be a further step for the client retrieving the key value from the cookie, executing a copy of the decryption engine, and decrypting the data. In some cases the server sends a copy of the encryption/decryption engine to the client, and this copy may be discarded after use. Also a new key may be sent for each session.

In another aspect of the invention a secure client/server system is provided, comprising a server having an encryption/decryption engine, access to data, and code

for sending a cookie to a user logging in to the server, and a client. The server, upon receipt of a data request by a client, sends a cookie to the client wherein the value of the cookie comprises an encryption/decryption key, and wherein the server encrypts the data requested by the client using the key before transmission to the client.

In preferred embodiments the client, after receiving encrypted data from the server, retrieves the key from the cookie value, and uses the key with the encryption/decryption engine to decrypt the data. In some cases the server sends a copy of the encryption/decryption engine to the client, and the copy may be discarded after use. In some cases a new key is sent each time a client logs in to the server.

In another aspect of the invention, in a client-server system, a method for encrypting data on a client from a server is provided, comprising steps of (a) upon receiving a log-in the client by the server, sending a cookie to the client, the cookie comprising a key value to be used for encryption the data, and sending an indication of the data to be encrypted; (b) accessing the key value by the client from the cookie sent; and (c) encrypting the data on the client using an encryption/decryption engine and the value of the key retrieved from the cookie value. In some cases the server sends a copy of the encryption/decryption engine to the client, and the copy may be discarded after use. Also a new key may be sent every session.

In yet another aspect a secure client/server system is provided, comprising a server having an encryption/decryption engine, access to data, and code for sending a cookie to a user logging in to the server; and a client. In this system the server, upon receipt of a log-in by a client, sends a cookie to the client wherein the value of the cookie comprises an encryption/decryption key, and sends also an indication of data to be encrypted, and wherein the client retrieves the key value from the cookie, and encrypts the data indicated by the server using the key. Again, in some cases the server sends a copy of the encryption/decryption engine to the client, and the copy may be discarded after use. Also a new key may be sent for each session.

In yet another aspect of the invention a method for secure data transfer between a first and a second server is provided, comprising steps of (a) the first server contacting the second server for data; (b) the second server sending a cookie to the first server, the value of the cookie comprising a key value for encryption/decryption;

(c) encrypting data before transmission by the second server, using the key value; and (d) sending the encrypted data to the second server. The second server may send a copy of an encryption/decryption engine to the first server, and the first server uses the copy with the retrieved key to accomplish decryption.

In various embodiments of the invention taught in enabling detail below, for the first time a secure means of data transfer is provided wherein keys for encryption and decryption are transferred as a part of a cookie.

Brief Description of the Drawing Figures

Fig. 1 is a block diagram illustrating a revolving encryption/decryption process initiated from a secure server on behalf of a client station according to an embodiment of the present invention.

Fig. 2 is a block diagram illustrating a revolving encryption/decryption process used in a server to server mode.

Fig. 3 is a flow diagram depicting a method of practicing the present invention.

Description of the Preferred Embodiments

In a preferred embodiment of the present invention, a unique method for encrypting, decrypting, and sending secure data over a data-packet network is provided that allows data to be automatically encrypted or decrypted under control of a sending node. Such a method is described in enabling detail below.

Fig. 1 is a block diagram illustrating a revolving encryption/decryption process initiated from a WEB server on behalf of a client station according to an embodiment of the present invention. A WEB server 67 is provided and adapted to function as an Internet file server as is known in the art. Server 67 may be adapted to provide portal

services, messaging services, HTTP services, Proxy services or any other known WEB service to clients who subscribe to such services, or to users in general.

A client station 79 is provided and adapted as an Internet capable appliance. That is, station 79 has enough memory, processing power, and suitable software for navigating the Internet and interacting with server 67. Client station 79 is adapted for accessing server 67 through any known means of Internet connection. It will be assumed here that the means used for connecting to server 67 is a standard modem/ISP-type Internet-access connection as is most common for public access.

Server 67 has a software log-in interface 71, which is provided and adapted to allow users access to any services offered. Log-in to server 67 from station 79 is illustrated herein by a directional arrow labeled *Log-in*. To gain access, a user must enter a user name and password as is typical in the art. Once logged in, a user may interact with server 67 according to services provided as is generally known in the art.

Server 67 has a data encryption/decryption software engine 73 provided therein and adapted to encrypt or decrypt any data stored in or controlled by server 67. In this example a user-data block 69 represents data that is requested by and designated to be sent to a user. Engine 73 is, in a preferred embodiment, a Java-based encryption/decryption program, many of which are known in the art and routinely used to encrypt and decrypt data. Engine 73 generates and uses an encryption/decryption key 75 for the purpose of encrypting or decrypting data as illustrated by a double arrow placed between elements 73 and 69. Key 75 is typically a line code generated for and used in conjunction with engine 73 for each encryption and decryption process. For example, data is encrypted according to the key, and must be decrypted according to the same key.

Server 67 has a "cookie" generator software engine provided therein and adapted for generating "cookies", which are text files known in the art typically used for tracking user navigation on the Internet. Typically a WEB site generates and sends a cookie to users who log-in or visit certain WEB pages held in and hosted by the server. Once a WEB cookie is sent to a user, it is stored in a user's machine-cache-memory and is returned to the server the next time a user logs in, as is well

known in the art. Only the hosting WEB site has control over generating a cookie for that WEB site.

A cookie in the art has typically both a name and a value, and the value may change each time a cookie is sent, again under control of the server. According to a preferred embodiment of the present invention, decryption key 75 is made to be the cookie value, or added or otherwise combined with or appended to the cookie value, becoming part of that value, and is sent to users for encrypting or decrypting data stored on their machines, or data sent to them from server 67.

In this example, client station 79 has data block 81 illustrated therein, which represents data block 69 after it has been received at client station 79. An encryption/decryption program 83 represents, in one embodiment, a temporary copy of program 73 after being sent from server 67 to station 79. Data-block 81 and engine 83 are downloaded to a user's WEB browser, represented by element number 82, after successful log-in. This is illustrated herein by the directional arrow labeled *Send Data/Program*. Data-block 81 may be any type of data that a user has requested from server 67. In another embodiment, encryption/decryption engine 83 may be resident at station 79, perhaps associated with WEB browser 82 as a plug-in.

A cookie 84, illustrated as residing in a Web cache 85 provided within station 79 represents a cookie containing the value of key 75. Key 75 is integrated into cookie 84 during cookie generation. Key 75, in this case, is a decryption key used for decrypting data block 81 at station 79, using engine 83.

In practice of the present invention, a user operating client station 79 logs into server 67 as illustrated by a directional arrow labeled *Log-in* proceeding from station 79 and progressing to log-in interface 71. Log-in interface 71 is adapted to prompt a user for a user name and password in order to verify identity and allow access to full services offered by server 67.

In one embodiment, once a user identity is properly confirmed and a data request is verified, server 67 encrypts all user-requested data represented by data block 69 using engine 73 as illustrated by a double arrow labeled *Encrypt*, and according to key 75. After encryption is completed, server 67 sends encrypted data block 69 and a temporary copy of encryption/decryption program 73 (if a user does

not already have one) to the user over the Internet as illustrated by a directional arrow labeled *Send Encryption Engine*. Received versions of block 69 and engine 73 are downloaded to browser 82 and appear as element 81 (user data) and element 83 (encryption/decryption engine) respectively.

Key 75, which is the key used for encrypting and decrypting user data 69 at server 67, is value-added to a text cookie generated by software 77 as illustrated by directional arrows proceeding from engine 73 to key 75 and then to generator 77. The cookie (cookie 84) is sent to client station 79 as illustrated by a directional arrow labeled *Send Cookie* where it resides as cookie 84 in WEB cache 85. It is noted herein that in one embodiment any data held in server 67 and targeted for sending to a user may be encrypted with a new key 75 every time the user logs-in to server 67 to access services. In another embodiment, encryption may be performed on a less frequent basis such as perhaps every 10 sessions or so. Any frequency may be applied.

After successful log-in to server 67 and data transfer, a user operating at station 79 now has all of his or her requested data in encrypted form, a program for decrypting the data, and a key for the program to use in automatically decrypting the data. Engine 83 automatically decrypts the received data 81 at client station 79 by retrieving cookie 84 from cache 85 as illustrated by a double arrow labeled *Retrieve Key*, accessing the key from the cookie value, and using the key in decryption. In this example, server 67 is first encrypting requested data and sending it to a client along with (if needed) a temporary encryption/decryption program and a key (in the cookie). The above-described method allows a user to be sure that no one will intercept and be able to decrypt data that he or she is receiving from a server. Moreover, only the issuing server may change the value of a cookie and key combination.

In another embodiment, server 67 may encrypt data on client station 79 for any purpose, such as for transmission over the Internet back to server 67 or, if server 67 is a proxy, by proxy to another server requiring the information for a transaction or the like. A transaction data-block 86 is illustrated within browser 82 at station 79 and represents any data that a user wants to send to a server. A transaction dialog box, represented herein by element 87, appears in browser window 82 during a transaction

process with a server as is typical and known in the art of WEB navigation. Box 87 may be a form requiring credit card or other sensitive information used to purchase an item or service.

In this example server 67 is presumed to be a proxy server and clear-text data in block 86 on client station 79 is first encrypted using engine 83 (downloaded from server 67) and cookie 84 (containing key 75). This process is illustrated by the double arrow labeled *Retrieve Key*, and a directional arrow proceeding from element 83 to element 86. Server 67 would also send an encryption/decryption program and a cookie containing key 75 to any WEB server transacting with a user operating station 79. This process is represented by a directional arrow labeled *WEB Service* illustrated at server 67. A target server (WEB service) receives encrypted data from station 79 as represented by a directional arrow labeled *WEB Service* illustrated at station 79. The WEB service also has key 75 and program 73 from server 67. Therefore, the target server is enabled to automatically decrypt the data from station 79 and for entry into a form field. The method and apparatus of the present invention may be used with any dialog or transaction interface presented by any WEB service.

In still another embodiment, server 67 may encrypt data at station 79 for transmission over the Internet back to server 67. In this embodiment, server 67 retains key 75 for the later decryption process. Security in all described embodiments is enhanced by virtue of the fact that the value of a cookie, including key 75, can only be changed by an issuing server and not by a third party. Moreover, key 75 is received in cache memory and cannot be manually manipulated for use with program 83 for decrypting or encrypting information. Server 67 may encrypt data differently each time a user logs on to receive data and send a new cookie/key combination, which overwrites the old one in cache thereby further enhancing security of data during transit. A new encryption/decryption program may be sent in conjunction with every new key such that when a user logs-off, the new encryption/decryption program is not retained.

According to yet another embodiment of the present invention, the method taught above may be practiced between two WEB servers running server software. Such an embodiment is described below.

Fig. 2 is a block diagram illustrating a revolving encryption/decryption process used in a server to server mode. In this example, two Internet servers are illustrated as WEB server 89 and WEB server 91. WEB server 89 is, for the purpose of this example, designated as the "sending" server while WEB server 91 is designated as the "receiving" server.

Server 89 has a resident encryption/decryption engine 95 provided therein and adapted for encrypting and decrypting data as was described with reference to Fig. 1. A data-block 93 illustrated within server 89 represents any data that is encrypted by virtue of engine 95 as illustrated by a double arrow labeled *Encrypt.* A decryption key 97 is illustrated within server 89 and represents a generated key for decrypting and encrypting data in block 93. Server 89 also has a communication interface 101, which is provided and adapted for communication with other servers. A cookie generator is also provided and adapted to generate and send cookies as is known in the art.

A data block 103 is illustrated within server 91 and represents encrypted data 93 received from server 89. Server 91 is, in this instance, in receiving mode. Server 91 has an encryption/decryption engine 105 illustrated therein and adapted for encrypting and decrypting data as illustrated by a double arrow labeled *Decrypt.* In one embodiment, engine 105 is a temporary program received from server 89 along with data 103. In this example server 89 would always be the controlling server. In another embodiment, server 91 may be adapted with full encryption/decryption and key generating capability such that neither server 89 or 91 is a controlling server.

Server 91, being the receiving server in this example, has a WEB cache 109 containing a WEB cookie 110 (received from server 89), and decryption key 97 retrieved from cookie 110 for data-decrypting purposes. Both servers have communication interfaces, interface 101 (for server 89) and interface 111 (for server 91) installed therein and adapted to allow communication over the Internet as known in the art.

Assume now that server 91 has established a connection-data request to server 89 through communication interface 111, over the Internet, to communication interface 101. After a communication connection is established between servers 89 and 91, data (93) is encrypted by encryption/decryption engine 95 using key 97 as

illustrated by the double arrow labeled *Encrypt*. Encrypted data 93 is sent to server 91 over the open connection (interface 101 to 111). The value of key 97 is integrated into a cookie generated by cookie generator 99 and sent to server 91 where it resides in cache 109 as WEB cookie 110. This is illustrated by directional arrows first starting at element 95 and proceeding ultimately to communication interface 101 at server 89, and by directional arrows starting at communication interface 111 at server 91 and proceeding ultimately to respective elements.

At server 91, encryption/decryption engine 105 retrieves key 97 from WEB cookie 110 in cache 109 as illustrated by double arrows placed between the involved elements. Engine 105 then uses key 97 to decrypt data 103 for use. In the above example, server 89 is the controlling server and issues temporary encryption/decryption programs and keys to servers requesting secure data. In this embodiment, data may be encrypted differently with a new key each time a server requests and is granted a connection for data transmission from the controlling server.

In another embodiment, server 89 may encrypt data held at another server for transmission back to itself by first sending program 105 and key 97 for the requesting server to encrypt data for transmission back. In this case, server 89 would retain a copy of key 97 for decryption purposes.

In still another embodiment, both servers 89 and 91 may be adapted as controlling servers such that each may send the other a temporary encryption program and a key for decryption. There are many possibilities.

The method and apparatus of the present invention may be practiced on any data-packet network that supports the use of cookies, Hyper-Text-Transfer-Protocol (HTTP) and other suitable Internet Protocol (IP) without departing from the spirit and scope of the present invention. For example, a business may use the method as a secure data transfer process on a corporate Local-Area-Network (LAN) or Wide-Area-Network (WAN).

In yet another embodiment, a controlling server adapted to send encryption/decryption programs and keys may multicast sensitive data to a plurality of receiving servers or client stations such that all the receivers get the same encrypted data securely without fear of intercept.

The method and apparatus of the present invention should be afforded the broadest scope possible in light of the several embodiments described. The spirit and scope of the present invention is limited only by the claims that follow.

What is claimed is:

1. In a client-server system, a method for encrypting and sending data from the server to the client and enabling decryption by the client, comprising steps of:

(a) upon receiving a log-in and a data request from the client by the server, sending a cookie to the client, the cookie comprising a key value to be used for decrypting the data;

(b) encrypting the data to be sent to the client using an encryption/decryption engine and the value of the key; and

(c) sending the encrypted data to the client.

2. The method of claim 1 further comprising a step for the client retrieving the key value from the cookie, executing a copy of the decryption engine, and decrypting the data.

3. The method of claim 1 comprising a step for the server sending a copy of the encryption/decryption engine to the client.

4. The method of claim 3 wherein the copy of the encryption/decryption engine is discarded after use.

5. The method of claim 1 wherein a new key is sent each time a client logs in to the server.

6. A secure client/server system, comprising:

a server having an encryption/decryption engine, access to data, and code for sending a cookie to a user logging in to the server; and

a client;

characterized in that the server, upon receipt of a data request by a client, sends a cookie to the client wherein the value of the cookie comprises an

encryption/decryption key, and wherein the server encrypts the data requested by the client using the key before transmission to the client.

7. The system of claim 6 wherein the client, after receiving encrypted data from the server, retrieves the key from the cookie value, and uses the key with the encryption/decryption engine to decrypt the data.

8. The system of claim 6 wherein the server sends a copy of the encryption/decryption engine to the client.

9. The system of claim 8 wherein the copy of the encryption/decryption engine is discarded after use.

10. The system of claim 6 wherein a new key is sent each time a client logs in to the server.

11. In a client-server system, a method for encrypting data on a client from a server, comprising steps of:

(a) upon receiving a log-in the client by the server, sending a cookie to the client, the cookie comprising a key value to be used for encryption the data, and sending an indication of the data to be encrypted;

(b) accessing the key value by the client from the cookie sent; and

(c) encrypting the data on the client using an encryption/decryption engine and the value of the key retrieved from the cookie value.

12. The method of claim 11 comprising a step for the server sending a copy of the encryption/decryption engine to the client.

13. The method of claim 12 wherein the copy of the encryption/decryption engine is discarded after use.

14. The method of claim 11 wherein a new key is sent each time a client logs in to the server.

15. A secure client/server system, comprising:

a server having an encryption/decryption engine, access to data, and code for sending a cookie to a user logging in to the server; and

a client;

characterized in that the server, upon receipt of a log-in by a client, sends a cookie to the client wherein the value of the cookie comprises an encryption/decryption key, and sends also an indication of data to be encrypted, and wherein the client retrieves the key value from the cookie, and encrypts the data indicated by the server using the key.

16. The system of claim 15 wherein the server sends a copy of the encryption/decryption engine to the client.

17. The system of claim 16 wherein the copy of the encryption/decryption engine is discarded after use.

18. The system of claim 15 wherein a new key is sent each time a client logs in to the server.

19. A method for secure data transfer between a first and a second server, comprising steps of:

(a) the first server contacting the second server for data;

(b) the second server sending a cookie to the first server, the value of the cookie comprising a key value for encryption/decryption;

(c) encrypting data before transmission by the second server, using the key value; and

(d) sending the encrypted data to the second server.

20. The method of claim 19 wherein the second server sends a copy of an encryption/decryption engine to the first server, and the first server uses the copy with the retrieved key to accomplish decryption.

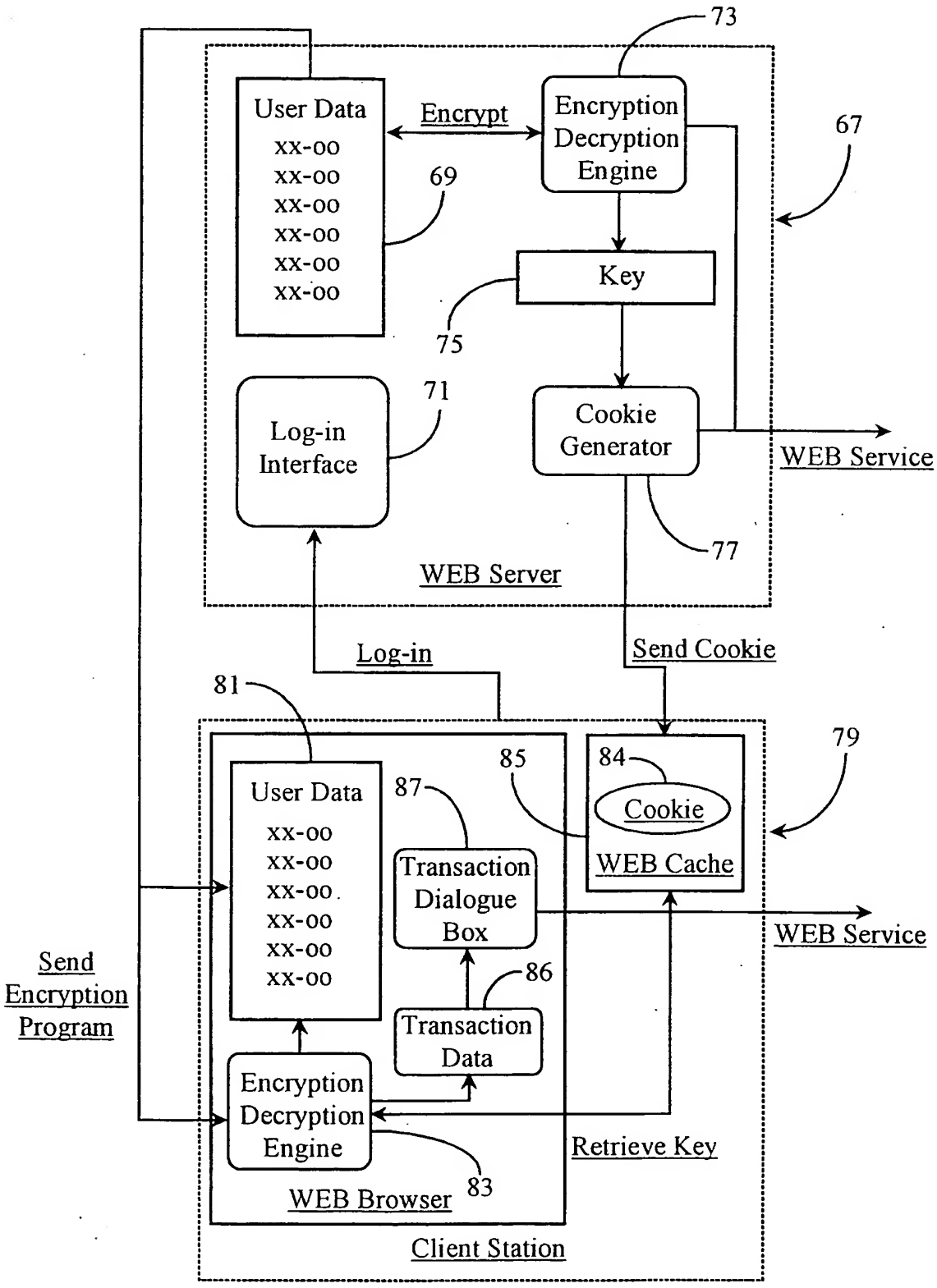

73
User Data
xx-oo
xx-oo
xx-oo
xx-oo
xx-oo
xx-oo
Encrypt
Encryption Decryption Engine
67
69
Key
75
Log-in Interface
71
Cookie Generator
WEB Service
77
WEB Server
Log-in
Send Cookie
81
79
85
84
Cookie
WEB Cache
87
User Data
xx-oo
xx-oo
xx-oo
xx-oo
xx-oo
xx-oo
Transaction Dialogue Box
WEB Service
Send Encryption Program
86
Transaction Data
Encryption Decryption Engine
Retrieve Key
83
WEB Browser
Client Station

Fig. 1

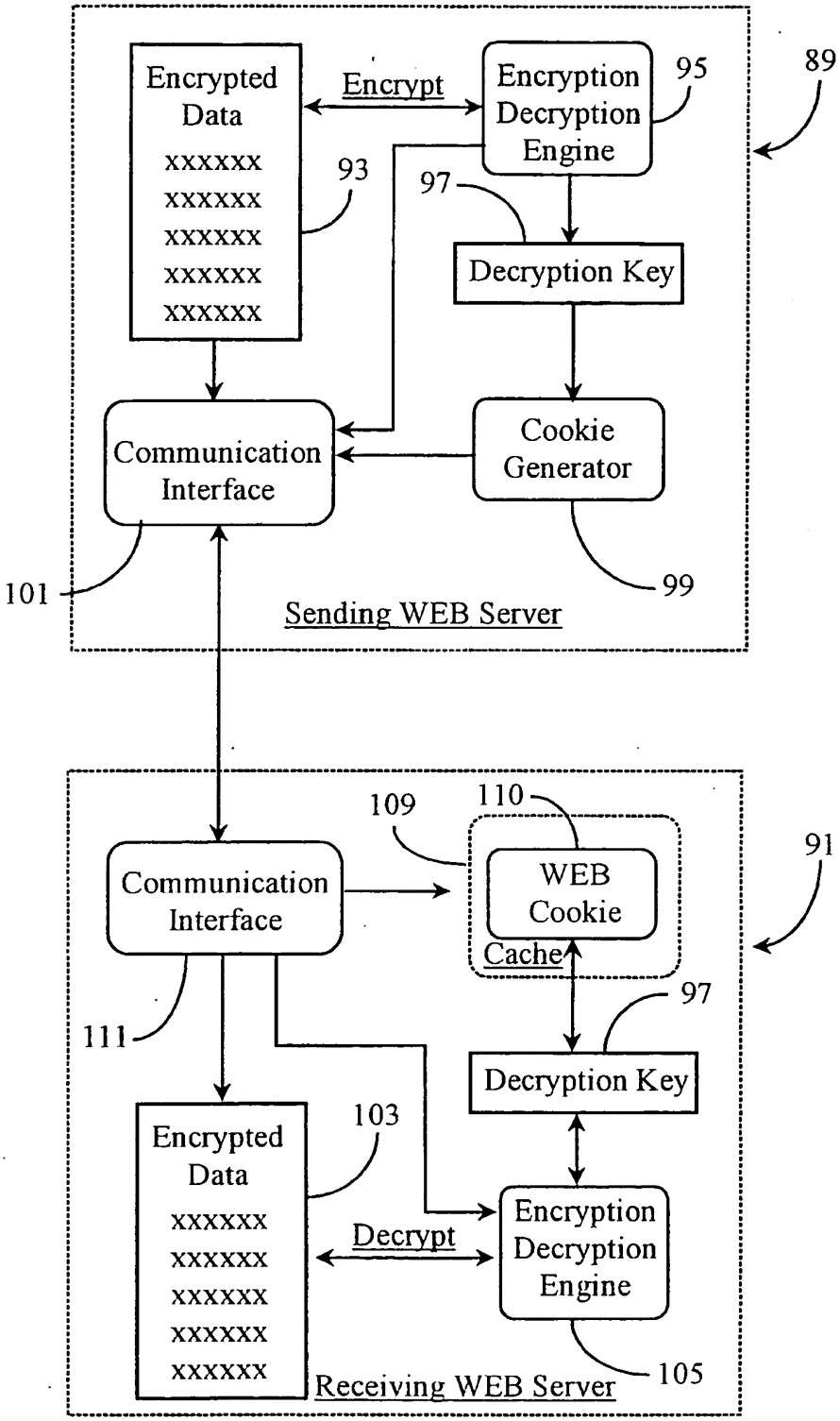

Encrypted Data
xxxxxx
xxxxxx
xxxxxx
xxxxxx
xxxxxx
Encrypt
Encryption Decryption Engine
95
89
93
97
Decryption Key
Communication Interface
Cookie Generator
99
101
Sending WEB Server
109
110
WEB Cookie
Cache
91
Communication Interface
111
97
Decryption Key
103
Encrypted Data
xxxxxx
xxxxxx
xxxxxx
xxxxxx
xxxxxx
Decrypt
Encryption Decryption Engine
105
Receiving WEB Server

Fig. 2

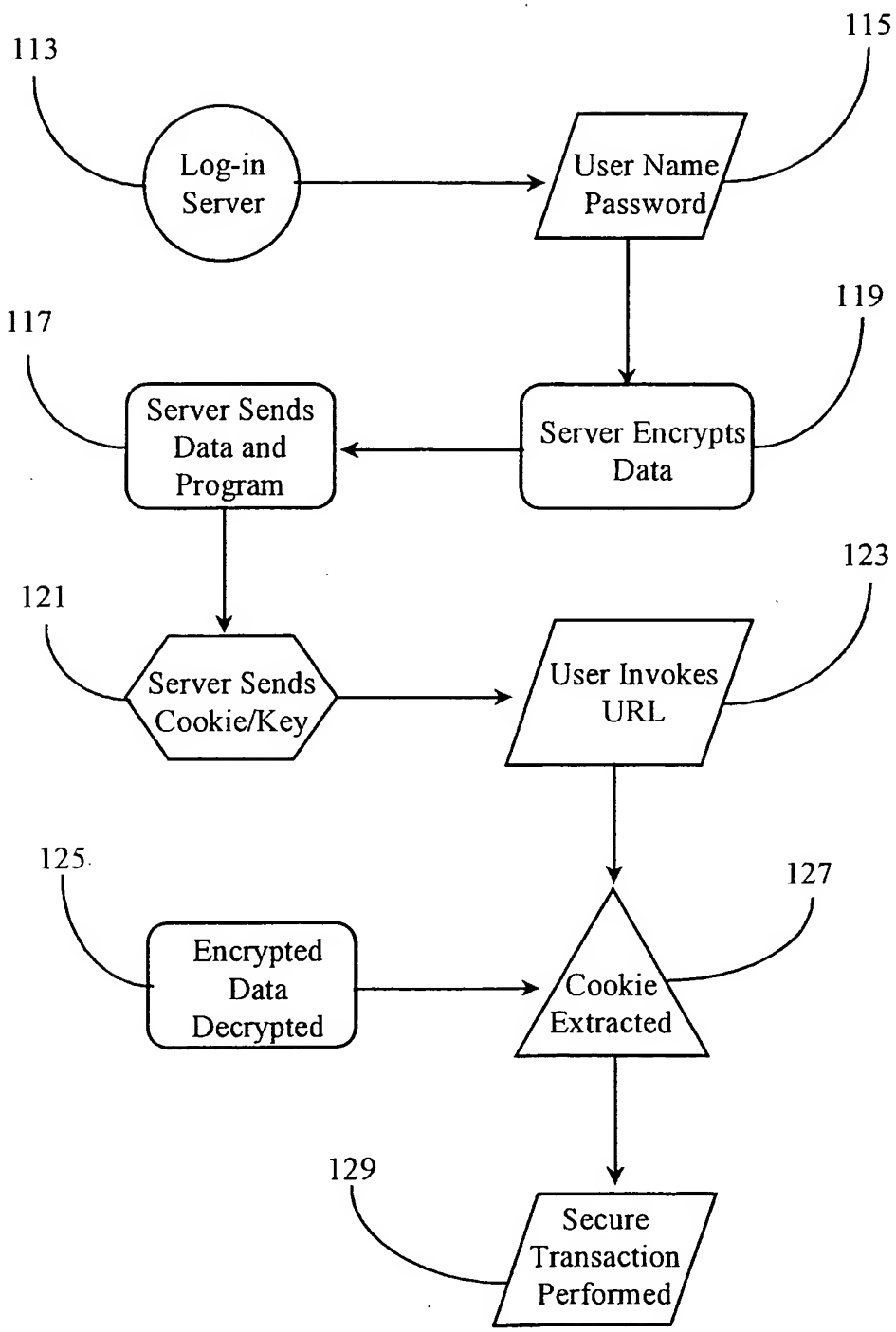

113
Log-in Server
115
User Name Password
119
117
Server Sends Data and Program
Server Encrypts Data
123
121
Server Sends Cookie/Key
User Invokes URL
125
127
Encrypted Data Decrypted
Cookie Extracted
129
Secure Transaction Performed

Fig. 3

INTERNATIONAL SEARCH REPORT

Inte ional application No.
PCT/US00/42168

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04L 9/12, 9/08
US CL : 380/260, 283
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 380/260, 283

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EAST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,E	US 6,226,750 B1 (TRIEGER) 1 May 2001, column 9, line 64 through column 10, line 13.	1-20
X,E	US 6,199,113 B1 (ALEGRE et al.) 6 March 2001, column 4, lines 32-44, column 5, lines 7-19.	1-20
Y	US 5,966,441 A (CALAMERA) 12 October 1999, column 12, lines 52-64.	1-20
Y	US 5,818,935 A (MAA) 6 October 1998, column 7, line 66 through column 8, line 9.	1-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
07 May 2001 (07.05.2001)	25 MAY 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Gilberto Barron, Jr. Peggy Harod Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet) (July 1998)